

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEIZURE OF)
CRYPTOCURRENCY IN THE MONERO)
WALLET DESCRIBED HEREIN AND)
FURTHER DESCRIBED IN)
ATTACHMENT A.)

No. 4:24MJ9129 RHH

FILED UNDER SEAL

SIGNED AND SUBMITTED TO THE
COURT FOR FILING BY RELIABLE
ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT

I, David J. Ogurek, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a seizure warrant for the

Subject **Account,** a Monero wallet with address

[REDACTED]

[REDACTED] with recovery phrase starting with “[REDACTED]” and ending with “[REDACTED]” associated with John Daniel CRUZ. This account, including any cryptocurrency stored therein, is subject to forfeiture under Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(7) and Title 28, United States Code, Section 2461 and therefore is subject to seizure under Title 18, United States Code, Sections 981(b) and 982(b) and Title 21, United States Code, Section 853(e) and (f) concerning violations of Title 18, United States Code, Section 371(conspiracy to commit offense), Title 21, United States Code, Section 331(b) (misbranding of a drug in interstate commerce), 331(a) (introduction of misbranded drugs into interstate commerce), and 331(i)(3) (c) (sale of a counterfeit drug); (“Subject Offenses”). I seek authorization to seize the items more fully set forth in **Attachment A**, including any cryptocurrency contained within the **Subject Account**.

2. I am a Special Agent with the (FBI), and I have worked as such for approximately seventeen (17) years. My current assignment is with the Violent Crime/Organized Crime Squad where I am detailed to work organized crime investigations and investigations related to illegal activity conducted on the Darknet. I have had numerous contacts and dealings with informants, victims, and other individuals known to engage in organized criminal activity, to include drug trafficking, major theft, money laundering, and fraud. I have investigated and/or assisted in numerous investigations relative to federal cases concerning the below-listed offenses. I have also received additional training in the illegal use of the Darknet to include the operations of Darknet Marketplaces (DNM), use of virtual currency, and the utilization of end-to-end encrypted communications applications.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 371 (conspiracy to commit offense), Title 21, United States Code, Section 331(b) (misbranding of a drug in interstate commerce), 331(a) (introduction of misbranded drugs into interstate commerce), and 331(i)(3) (c) (sale of a counterfeit drug) have been committed by John Daniel CRUZ, others known and unknown, and evidence and fruits of those crimes is located on the **Subject Account**.

5. As set forth below, there is probable cause to believe that CRUZ committed and is continuing to commit the Subject Offenses. The **Subject Account** is used by CRUZ in furtherance of the Subject Offenses and is used to store the proceeds from the sale of counterfeit/misbranded

drugs on the DarkNet. There is also probable cause to seize the Subject Account as evidence of these crimes and contraband or fruits of these crimes.

FORFEITURE AUTHORITY

6. Pursuant to 18 U.S.C. 982(a)(7), any property, real or personal, that constitutes or is derived, directly or indirectly, from gross proceeds traceable to the commission of a Federal health care offense are subject to criminal forfeiture. The term “Federal health care offense” includes violations of 21 U.S.C. § 331. See 18 U.S.C. § 24(a)(2).

7. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461, any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting “specified unlawful activity” is subject to both civil and criminal forfeiture. The term “specified unlawful activity” includes violations of 21 U.S.C. § 331. See 18 U.S.C. § 1956(c)(7)(F).

8. Pursuant to 18 U.S.C. § 981(b), property subject to civil forfeiture may be seized by a civil seizure warrant issued by a judicial officer “in any district in which a forfeiture action against the property may be filed,” and may be executed “in any district in which the property is found,” if there is probable cause to believe the property is subject to forfeiture. A civil forfeiture action may be brought in any district where “acts or omissions giving rise to the forfeiture occurred.” 28 U.S.C. § 1355(b)(1)(A). As detailed below, acts or omissions under investigation occurred in the Eastern District of Missouri. 21 U.S.C. § 853(f) provides authority for the issuance of a seizure warrant for property subject to criminal forfeiture.

9. Based on the foregoing, the issuance of this seizure warrant is authorized under 21 U.S.C. § 853(f) for criminal forfeiture; and 18 U.S.C. § 981(b) for civil forfeiture. Notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, the issuance of this seizure

warrant in this district is appropriate under 18 U.S.C. § 981(b)(3) and 28 U.S.C. § 1355(b)(1) because acts or omissions giving rise to the forfeiture occurred in the Eastern District of Missouri.

**BACKGROUND CONCERNING THE DARKNET
AND VIRTUAL CURRENCY**

10. The “dark web,” or “Darknet,” is a portion of the “deep web” of the Internet, where individuals must use an anonymizing software or application to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the “clear web” or simply the “web”). These marketplaces are known as “hidden services” and use web extension “.onion.” They are called hidden services because, by their nature, neither the operator of the site nor the visitor knows each other’s true IP address. This makes locating the physical locations of the servers very difficult. To access the dark web, users must only install and use a web browser known as The Onion Router, or TOR.

11. “Vendors” are the dark web’s sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of “vendor accounts” on dark web marketplaces. Customers, meanwhile, operate “customer accounts.” Vendor and customer accounts are not identified by numbers, but rather monikers or “handles,” much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as “trusted” vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time.

12. Dread is a Darknet forum site similar to the clear website “Reddit.” Dread is commonly used as a forum to discuss illegal activities such as the manufacturing of drugs, sale of drugs, and ways to avoid law enforcement. Users can maintain “sub-dread” pages on Dread, which are similar to home pages.

13. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Cryptocurrency is not illegal in the United States.

14. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”).

A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’s private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

15. Bitcoin (“BTC”) is a type of cryptocurrency.¹ Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. Individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. It is also possible to earn bitcoin by verifying other users’ transactions, a process known as “mining.” Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it’s not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems. To transfer bitcoin to another address, the payor transmits a transaction announcement, cryptographically signed with the payor’s private key, across the peer-to-peer Bitcoin network. The Bitcoin address of the receiving party and the sender’s private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any

¹ Since Bitcoin is both a currency and a protocol, capitalization differs. Uppercase Bitcoin will denote protocol, software, and community whereas lowercase bitcoin will denote units of the currency.

identifying information. As a result, little-to-no personally identifiable information about the payor or payee is transmitted in a Bitcoin transaction itself. Once the payor's transaction announcement is verified, the transaction is added to the blockchain, a decentralized public ledger that records all Bitcoin transactions. The blockchain logs every Bitcoin address that has ever received a bitcoin and maintains records of every transaction for each Bitcoin address. Virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.

16. Monero ("XMR") is a type of cryptocurrency that uses a blockchain with privacy-enhancing technologies to obfuscate transactions in order to achieve anonymity. Unlike most other cryptocurrencies, Monero's users are anonymous by default. Generally speaking, observers cannot decipher addresses transacting XMR to learn transaction amounts, address balances or transaction history.

17. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or on websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an

address and a QR code with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (seemingly random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies are further secured, in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

18. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users’ funds or the private keys that are necessary to access users’ wallet applications. Rather, the private keys are stored on the specific device on which the wallet application was installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users’ cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user’s wallet directly, such as by accessing the user’s smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (further detailed below), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

19. Under the Federal Food, Drug, and Cosmetic Act (FDCA), Title 21, United States Code, Sections 301 et seq., the term “drug” includes any article intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or animals, or an article (other than food) intended to affect the structure or function of the body of man or other animals. 21 USC § 321(g)(1).

20. Alprazolam is a benzodiazepine used to treat anxiety disorders. Alprazolam is assigned to Schedule IV of the Controlled Substances Act and is available only by prescription. Pfizer Pharmaceuticals markets its pills containing alprazolam under the brand name Xanax. Several companies sell generic versions of Xanax. These generic versions are stamped with identifying numbers assigned by the National Drug Code such as, “B707” supplied by Breckenridge Pharmaceutical, Inc., “2090” supplied by Qualitest Pharmaceutical, Inc., and “S903” supplied by Dava Pharmaceutical, Inc. Bromazolam and clonazolam are both benzodiazepine derivatives. Bromazolam is not a scheduled substance. Clonazolam has temporary placement as a Controlled Substance as of July 26, 2023, until July 26, 2025. Neither are ingredients in Xanax.

21. All of the substances mentioned in this affidavit meet the statutory definition of drug. The introduction or delivery for introduction into interstate commerce of any misbranded drug is prohibited. 21 USC § 321(a). Misbranding encompasses dispensing without a valid prescription a drug intended for use by man which, because of its toxicity or potential harmful effect, was not safe for use except under supervision of a licensed practitioner or where its FDA-approved application limited it to prescription use. 21 USC § 353 (b)(1). Misbranding also occurs when the drug was manufactured, prepared, propagated, compounded, or processed in an establishment not registered with the Secretary of Health and Human Services. 21 USC § 352(o).

PROBABLE CAUSE

22. The Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Homeland Security Investigations (HSI), and United States Postal Inspection Service (USPIS), conducted a criminal investigation of CRUZ which led to his indictment in this district on March 1, 2023, for conspiracy to misbrand, introduce misbranded drugs, and sell counterfeit drugs in violation of Title 18 U.S.C. Section 371. United States v. Cruz, 4:23CR84 AGF. CRUZ pled guilty to the indictment on November 29, 2023 and is scheduled to be sentenced on May 10, 2024. As noted in the indictment, CRUZ conspired with others from at least November 2019 through July 2021, to manufacture, acquire, and sell misbranded drugs, essentially counterfeit and generic equivalents of Xanax, both with alprazolam and with bromazolam or clonazepam.

Identification of fortunecookiez

23. In 2021, the FBI arrested a DarkNet vendor manufacturing and selling counterfeit Xanax. The vendor used a pill press with imprint stamps that are substantially indistinguishable from those used by pharmaceutical companies selling generic forms of Xanax. Investigators discovered that CRUZ used the moniker **fortunecookiez** and on an encrypted communication application placed multiple large orders with the vendor. In communications with the DarkNet vendor, **fortunecookiez** directed that the counterfeit Xanax be shipped to “John Cruz” at 10 Alpine Street, #25, Rochester, New York. Investigators determined that CRUZ resided at the apartment listed on these DarkNet orders.

24. A review of United States Postal Service business records revealed that CRUZ, at this residence, received multiple large packages of counterfeit Xanax from the DarkNet vendor.

25. Investigators learned of a telephone number provided by CRUZ to American Airlines. According to records obtained from Verizon on the telephone number, the listed subscriber was “**FortuneCook**”.

New Post-Indictment Conspiracy

26. As previously noted, CRUZ was indicted for his role in the counterfeit Xanax conspiracy. On or about April 14, 2023, a bond hearing was conducted and CRUZ was granted pre-trial release. CRUZ was permitted to return to his residence in Rochester, New York.

27. In June 2023, a source (CS-1) sent an email to the DEA in St. Louis, Missouri regarding CRUZ. CS-1 stated they had seen a press release about the arrest of CRUZ, but CRUZ was still selling Xanax pills on a darknet onion site that he created. CS-1 further stated CRUZ had a team working for him. Investigators promised CS-1 that the cooperation with authorities would be relayed to state prosecutors in relation to a charged state crime. No further benefits were provided to CS-1.

28. Independently, HSI arrested a subject in [REDACTED] (CS-2) who also knew of CRUZ's operation. The information provided by CS-2 was consistent with the information provided by CS-1. Investigators promised CS-2 that the cooperation with authorities would be relayed to state prosecutors in relation to a state crime pending charges. No further benefits were provided to CS-2.

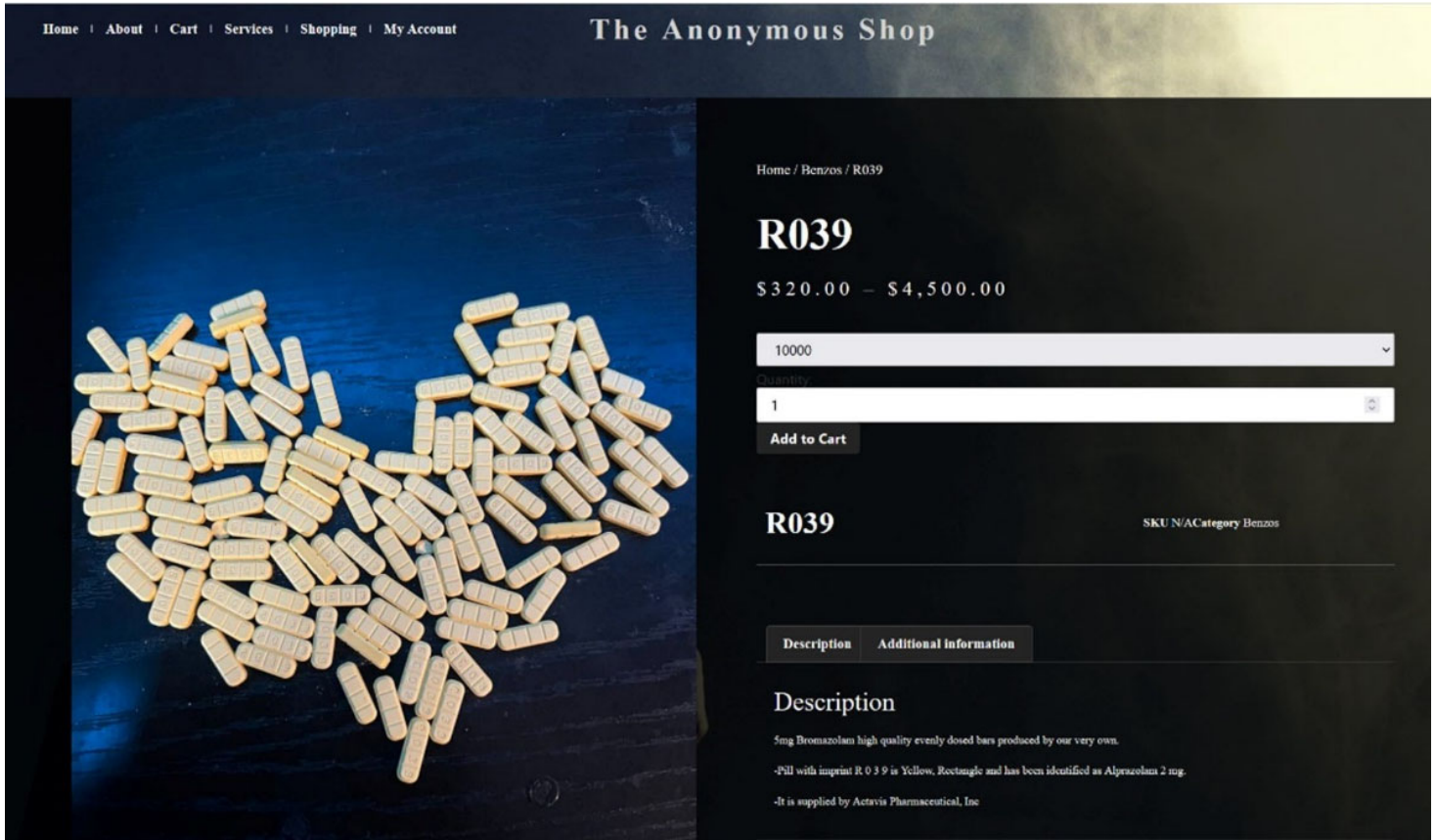
29. CS-1 stated that CRUZ has two pill pressing machines and is capable of producing 20,000 pills per hour. CRUZ has an associate known only to CS-1 as "Help," who operates the pill press machines and the shipping operations. According to CS-1, CRUZ oversees the operations via Ring web cameras.

30. CS-1 stated CRUZ was now using the online moniker "XMRMASTR." CS-1 provided the "onion" address for CRUZ's darknet website along with a login for the site. Investigators utilized the TOR browser and the provided login to access the site. The website is

titled “The Anonymous Shop.” On the “About” page, the site states it was designed by “XMRMASTR.”



31. The site offers four different varieties of counterfeit Xanax pills. The listing for each pill provides a photo and a description that provides the type and amount of active ingredient it is made with, a description of the imprint, color, shape, amount of the active ingredient in the legitimate pill, and the name of the pharmaceutical company who produces the legitimate version of the pill.



32. On September 26, 2023, an undercover investigator (UC-1) accessed CRUZ's darknet website using the login provided by CS-1 and made a purchase of 500 yellow "R039" pills for \$320.00. Payment for the pills was made with Bitcoin via a Bitcoin payment service on the site.

My Account

[Dashboard](#)[Orders](#)[Downloads](#)[Addresses](#)[Account Details](#)[Logout](#)

Order # 32 was placed on September 23, 2023 and is currently Shipped.

Order Details


Product	Total
R039 - 500 × 1 Size: 500	\$320.00
Subtotal:	\$320.00
Shipping:	Free shipping
Payment method:	BTCPay (Bitcoin, Lightning Network, ...)
Total:	\$320.00


33. On October 10, 2023, USPS Postal Inspector Nathalie Saputa intercepted a package shipped to the address provided by the UC containing one vacuum sealed bag containing multiple yellow rectangle-shaped pills with “R039” stamped on the pills. The pills were consistent with the pills offered on CRUZ’s darknet website and ordered by the undercover investigator. The package had a return address of “Sniffy Labs Inc., 125 Tech Park Dr., Rochester, NY 14623.” Laboratory analysis revealed that the pills contained Bromozalam and were misbranded.



34. On March 4, 2024, UC-1 again accessed CRUZ's darknet website and made a purchase of 5,000 "R039" pills and 5,000 "U94" pills for a total of \$4,500.00.

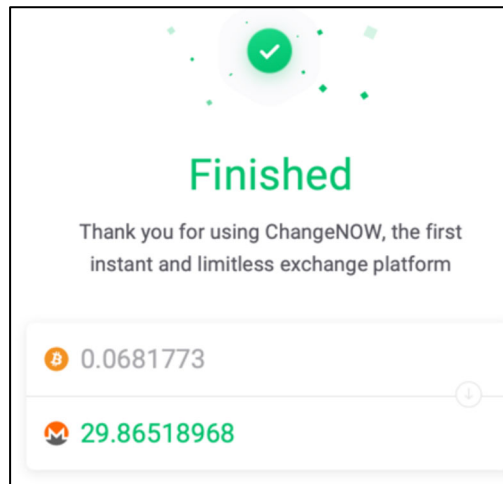
Product	Subtotal
R039 - 5000 × 1	\$2,400.00
U94 - 5000 × 1	\$2,400.00
Subtotal	\$4,800.00
Shipping	Free shipping
Discount	-\$300.00
Total	\$4,500.00

 BTC Pay (Bitcoin, Lightning Network, ...)

 BTC PAY

You will be redirected to BTC Pay to complete your purchase.

Payment for the pills was made with Monero via a Monero payment service on the site. The total amount of cryptocurrency sent was 29.86518968 XMR.



Connection Between Subject Offenses and Subject Account

35. On March 11, 2024, a package being sent to the address provided by the UC in this purchase was intercepted by investigators. The package contained pills matching the UC's order. The pills have been sent for laboratory analysis, which is pending.

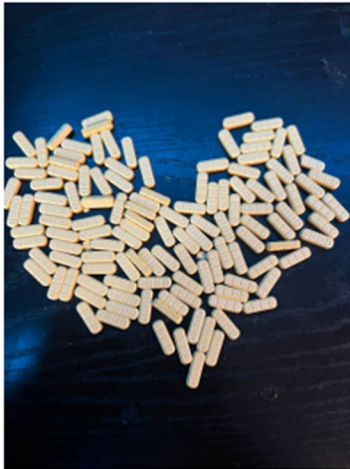
36. Pursuant to a federal grand jury subpoena, Apple produced account data associated with CRUZ's cellular telephone number and physical device. On or about November 2, 2023, Apple provided the following information:

- a. CRUZ's cellular telephone number was listed on iCloud accounts **fortunecookiez@icloud.com**.
- b. CRUZ's residence at [REDACTED] New York was listed on the **fortunecookiez@icloud.com** account.
- c. An Apple iPhone 12 PROMAX with IMEI 356717110628871 logged in to **fortunecookiez@icloud.com**.
- d. An iPad Mini 64GB with IMEI 351629570292707 logged in to **fortunecookiez@icloud.com**.

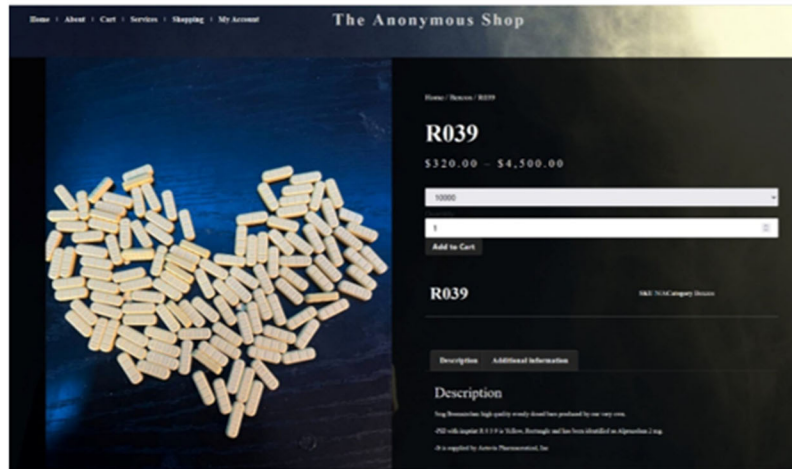
37. A federal search warrant was obtained for the content of the **fortunecookiez@icloud.com** account.

A review of the content of **fortunecookiez@icloud.com** revealed the following:

- a. Numerous photographs were saved on the iCloud drive depicting Xanax pills. One such image, as depicted below, is the exact photograph that appeared on the Anonymous Shop page:



fortunecookies@icloud.com
Search Warrant Data



Anonymous Shop Posting

- b. In another file, a video was captured wherein an individual had a small bag of Xanax bars taped to a toy mail truck. The video captured the toy mail truck driving to a toy mail box and dropping off the Xanax.



- c. Saved within the same folder in the iCloud drive, was a file named “fortunexmr.keys”, a picture file with the recovery seed phrases named “fortunexmr.png”, and a text file named “wallet.txt” that contained a wallet password.

d. The recovery seed phrase in “fortunexmr.png” is depicted below:

Write down your recovery phrase

These words are a backup of your wallet. Write these words down now on a piece of paper in the same order displayed. Keep this paper in a safe place and do not disclose it to anybody! Do not store these words digitally, always use a paper!

Recovery phrase (mnemonic seed): ⓘ

1 hornet	6 onward	11 dogs	16 espionage	21 eggs
2 ferry	7 hive	12 code	17 galaxy	22 null
3 adapt	8 upload	13 mailed	18 inexact	23 saxophone
4 gusts	9 against	14 sipped	19 soya	24 seventh
5 boldly	10 oasis	15 slower	20 hull	25 seventh

Creation date: 02/09/2023

Restore height: ⓘ 2945000

Print a template

Previous ● ● ● ● Next

38. I am aware from training and experience that cryptocurrency wallets can be accessed using a program named “GUI Wallet.” The program provides the user the ability to type in recovery seed phrases and save cryptocurrency wallets in a file with a “.keys” extension.

39. Utilizing the GUI Wallet program, investigators opened the “fortunexmr.keys” and used the password contained in “wallet.txt”. The file accessed a Monero wallet, with primary address the **Subject Account**.

40. As of April 8, 2024, the balance of the **Subject Account** was 1146.513248634792 XMR. The approximate value of the **Subject Account** was \$151,882.17 United States Dollars.

41. A review of the transactions for the **Subject Account** revealed that the first transaction occurred on or about September 27, 2023.

42. Further review of the **Subject Account**’s transactions revealed that it received 29.86518968 XMR on or about March 4, 2024. This amount corresponds to the March 4, 2024,

undercover purchase of counterfeit Xanax from the Anonymous Shop website and payment sent through the website's payment server. (See paragraph 34)

43. Based upon the foregoing, probable cause exists that CRUZ utilized the **Subject Account** in furtherance of the subject offenses and that the **Subject Account** contains evidence (transaction records) and fruits (cryptocurrency proceeds) of the subject offenses.

CONCLUSION

44. I respectfully submit that there is probable cause to believe that the **Subject Account**, including any cryptocurrency stored within, constitutes proceeds of violations of 21 U.S.C. § 331, are therefore subject to civil and criminal forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 982(a)(7), and 28 U.S.C. § 2461.

45. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under penalty of perjury that the foregoing is true and correct.



DAVID J. OGUREK
Special Agent
Federal Bureau of Investigation (FBI)

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 15th day of April 2024.

/s/ David D. Noce

HONORABLE DAVID D. NOCE
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A
Property to be Seized

Any and all cryptocurrency contained within the Subject Account.